DISCLAIMER: IF YOU DECIDE TO PERFORM THE FOLLOWING INSTRUCTIONS, YOU ACKNOWLEDGE THAT YOU'RE TAKING FULL RESPONSIBILITY FOR YOUR ACTIONS AND POSSIBLE CONSEQUENCES. ALWAYS EXERCISE CAUTION WHEN MODIFYING OPERATING SYSTEM SETTINGS.

Disable automated Windows Updates via Local Policy:

1. Open **gpedit.msc**
2. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Windows Update > Manage end user experience**
3. Set **Configure Automatic Updates** to **Disabled**
4. Optionally in the same location, you can also set **Remove access to use all Windows Update features** to **Disabled**. This effectively makes the Windows Update buttons in the system settings inactive and impossible to trigger by the user, either accidentally or on purpose.

Disable lingering services:

After applying the Local Policy config described above, the updates should be effectively stopped. If for whatever reason you'd like to "harden" it even more invasively and physically stop the update services from running idly in the background, you can do the following:

Disable scheduled tasks related to Update Services:

This will prevent UsoSvc (which we'll disable later) from being reset back to stock settings.

Tasks that need to be disabled are unfortunately protected, such that only NT AUTHORITY\SYSTEM account has full access to modify them. We need to disable them from that account's security context. Luckily, Task Scheduler itself allows us to create tasks that will run with any privilege level, including that of SYSTEM's account!

Open **taskschd.msc**

1. In any folder (i.e directly inside \Microsoft) create a new task.
2. On the **General** tab, in the **Security options** section click on the **Change User or Group** button. Inside the search box in newly opened window type`SYSTEM`and click the **Check Names** button. This should automatically find the full name of SYSTEM account and fill the rest of the field for you. Confirm the settings by clicking **OK** to close the dialogue.

3. Back at the General tab, tick the **Run with highest privileges** box.
4. Now, onto the **Actions** tab. Create a new action, and in the config window set the action type to ***Start a program.*** In the **Program/script** field type **powershell.exe.**
5. Now, in the **Add arguments (optional):** field type the following, replacing the [YOUR_USERNAME] with your actual user name:

   ```
   Get-ScheduledTask -TaskPath \Microsoft\Windows\
   UpdateOrchestrator\, \Microsoft\Windows\WaaSMedic\ |
   Disable-ScheduledTask >> "C:\Users\[YOUR_USERNAME]\
   Desktop\pslog.txt"
   ```

   The *>> "C:\Users\[YOUR_USERNAME]\Desktop\pslog.txt"* are optional commands, but they will let us see the output of the poweshell (in case of possible errors) by creating and writing to the pslog.txt file on the desktop. Remember that the script will run as SYSTEM account, while our active interactive session is that of currently logged in user, thus we won't get to see any GUI belonging to stuff running in SYSTEM session.

6. Confirm all the above settings by clicking **OK**.
   As the last step, on the **Trigger** tab, add any kind of trigger. it doesn't really matter what you set there, as we'll launch this task manually. For example you can set some date in the past as the trigger. It's necessary because with nothing specified, the task config dialog won't let us proceed.

7. Finally, confirm all the settings by clicking **OK** in the **Create Task** window.
   Back in the main Task Scheduler window, right click our newly created task and click **Run.**

This should have completely disabled all tasks located within `UpdateOrchestrator` and `WaaSMedic`folders. If any errors occured, you should be able to see them, written to the pslog.txt file on your desktop.

Set the UsoSvc service startup type to Disabled:

We can finally disable the very service that manages updates in the background. Open Powershell as an Administrator, and type the following:

```
Set-Service -Name UsoSvc -StartupType Disabled
Set-Service -Name wuauserv -StartupType Disabled
```

Final note: Disabling the services as described above, WILL render the Windows Update menu completely inaccessible, displaying an error. This is the expected behaviour when the relevant services aren't running.

Reverting all changes to default:

If you ever need to revert to the original system settings, just replace the *`Disable-ScheduledTask` with `Enable-ScheduledTask`* in the previously created task and re-run it to enable all update services.

Then, in Poweshell terminal with Administrator privileges run:

```
Set-Service -Name UsoSvc -StartupType Automatic
Set-Service -Name wuauserv -StartupType Automatic
```

References:
https://gpsearch.azurewebsites.net/Default.aspx?PolicyID=13564#2791
https://gpsearch.azurewebsites.net/Default.aspx?PolicyID=13564#13564
https://netwrix.com/en/resources/blog/how-to-automate-powershell-scripts-with-task-scheduler/
https://learn.microsoft.com/en-us/powershell/module/scheduledtasks/disable-scheduledtask?view=windowsserver2025-ps
https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/set-service?view=powershell-7.6